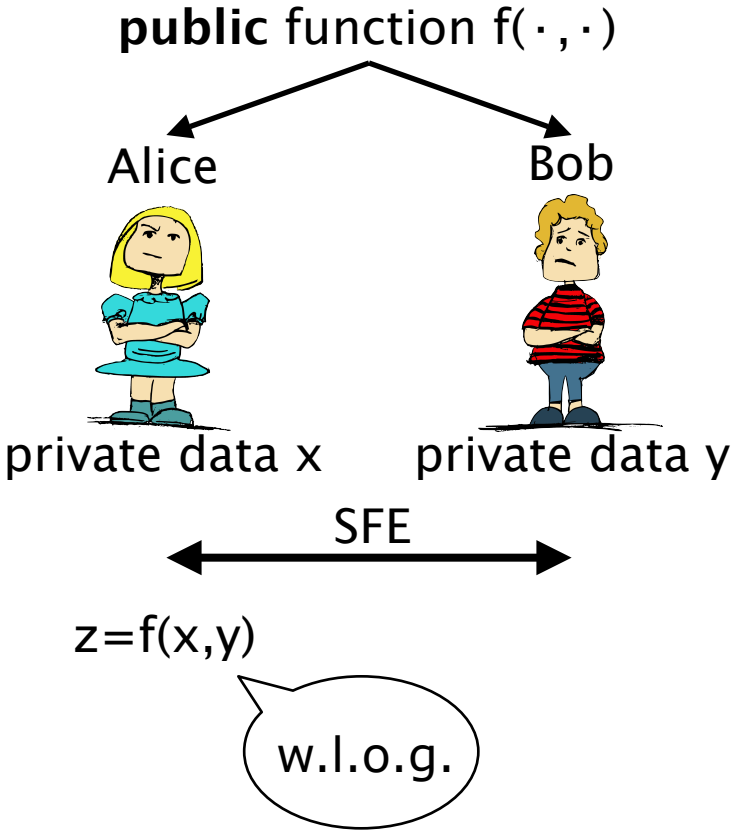
Improved Garbled Circuit Building Blocks and Applications to Auctions & Computing Minima

Ahmad-Reza Sadeghi, Thomas Schneider
Ruhr-University Bochum, Germany

Vladimir Kolesnikov
Alcatel-Lucent Bell Labs, USA

Secure 2-Party Computation (S2PC)

= Secure Function Evaluation (SFE)



e.g.,
- Millionaire's problem x<y
- Auctions
- Biometric Authentication (Face Recognition)

In the following: all parties **semi-honest**
(= honest-but-curious = passive adversaries)

Outline

- Two Paradigms for Secure 2-Party Computation
  - Homomorphic Encryption (HE)
  - Garbled Circuits (GC)
- How to combine HE and GC efficiently
- Efficient Circuit Constructions
- Improved Applications
  - Millionaire's Problem, Auctions, Minimum Distance
  - Outlook: Privacy-Preserving Face Recognition

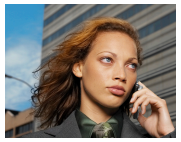
Paradigm 1: Homomorphic Encryption (HE)

Property: $\forall x, y \in P : \mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{pk}}(x) \circ_{\mathsf{pk}} \mathsf{Enc}_{\mathsf{pk}}(y)) = x \diamond y$

Some Schemes:

+	Paillier99 Damgård/Jurik01 Damgård/Geisler/Krøigård07	(default) (large P) (tiny P)
+, 1 *	Boneh/Goh/Nissim05	
+, *	Gentry09	

Application: S2PC by Computing on Encrypted Data



Paradigm 2: Garbled Circuits (GC) [Yao86]

Client 

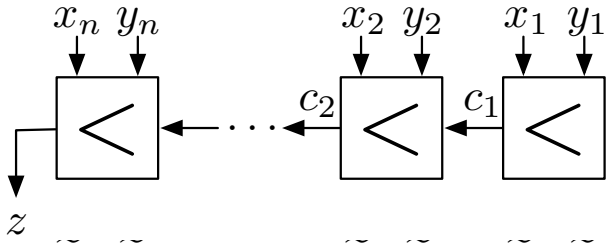
$f(\cdot,\cdot)$ e.g., $\mathbf{x} < \mathbf{y}$

Server 

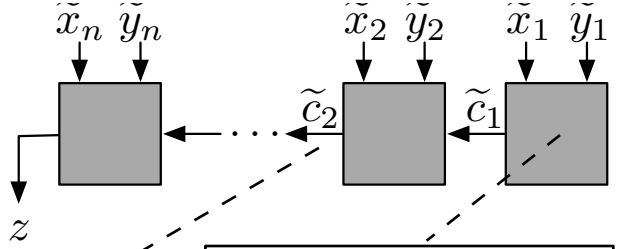
private data $\mathbf{x} = x_1, .., x_n$

private data $\mathbf{y} = y_1, .., y_n$

- Circuit



- Garbled Circuit $\widetilde{C}$



$\widetilde{C}, \widetilde{y}_1, \ldots, \widetilde{y}_n$

$\forall 1 \leq i \leq n : OT(x_i;\ \widetilde{x}_i^0, \widetilde{x}_i^1)$

$\widetilde{w}_i^0, \widetilde{w}_i^1$

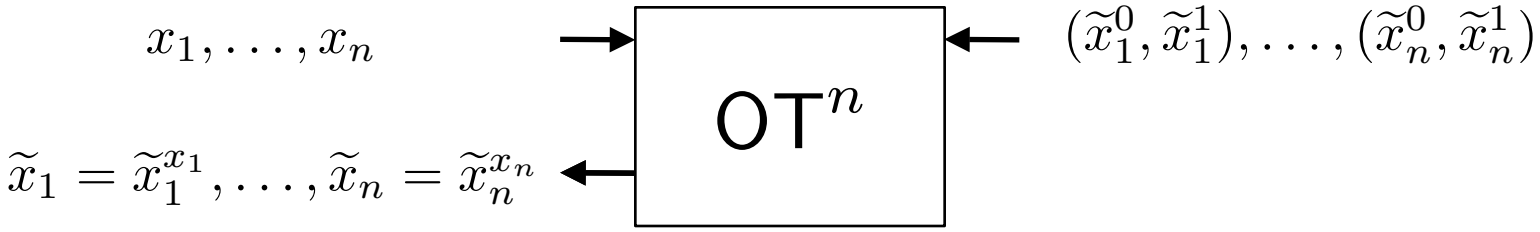
Garbled Wires

$$E(\widetilde{x}_1^0, \widetilde{y}_1^0;\ \widetilde{c}^{g(0,0)})$$
$$E(\widetilde{x}_1^0, \widetilde{y}_1^1;\ \widetilde{c}^{g(0,1)})$$
$$E(\widetilde{x}_1^1, \widetilde{y}_1^0;\ \widetilde{c}^{g(1,0)})$$
$$E(\widetilde{x}_1^1, \widetilde{y}_1^1;\ \widetilde{c}^{g(1,1)})$$

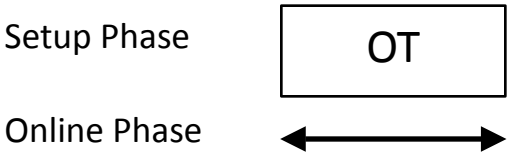
Garbled Table

$f(x, y) = \widetilde{C}(\widetilde{\mathbf{x}}, \widetilde{\mathbf{y}})$

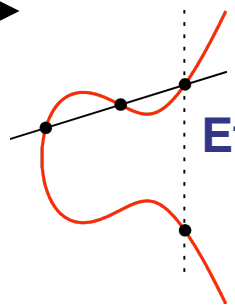
Parallel Oblivious Transfer (OT) is Efficient



Pre-computing OT [Bea95]



Non-Interactive OT with Trusted HW
[GT08], [Gol08]



Efficient OT protocols
[NP01], [AIR01], ...

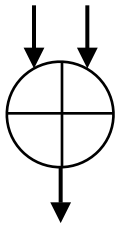
Extending OT efficiently [IKNP03]

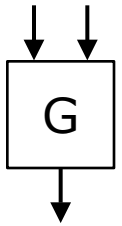
$$\mathsf{OT}^n \leftarrow \mathsf{OT}^t + \text{symmetric crypto}$$

Garbled Circuits are Efficient

Combine Several Techniques for Efficient GCs:

- Point-and-Permute [MNPS04]
- High-Speed Evaluation of GC [LPS08]
- Free XOR [KS08]





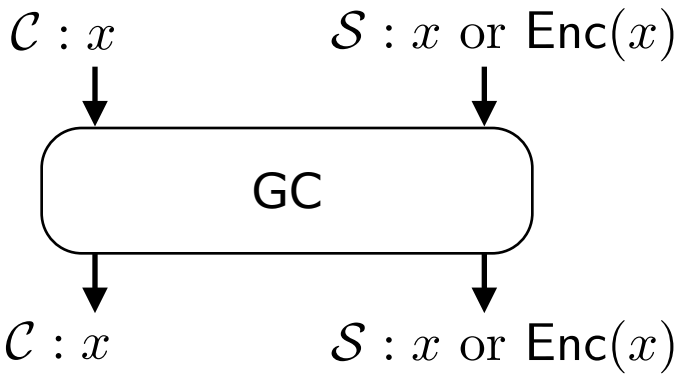
Even better (not in paper)
- Garbled Row Reduction [NPS99, PSSW09]: 3t' bits
- Secure HW Token (coming soon): 0 bits

Communication (offline)	0 bits	4t' bits
Computation	0	

	StM	ROM
Server (offline)	8 hash	4 hash
Client (online)	2 hash	1 hash

t=t'-1: symmetric security parameter (e.g., t=80)
hash: hash one block with cryptographic hash function

Paradigm 1+2: Combining HE with GC



Communication complexity to convert ℓ-bit values x for GC
(σ: statistical security parameter, $t' - 1$: symmetric security parameter)

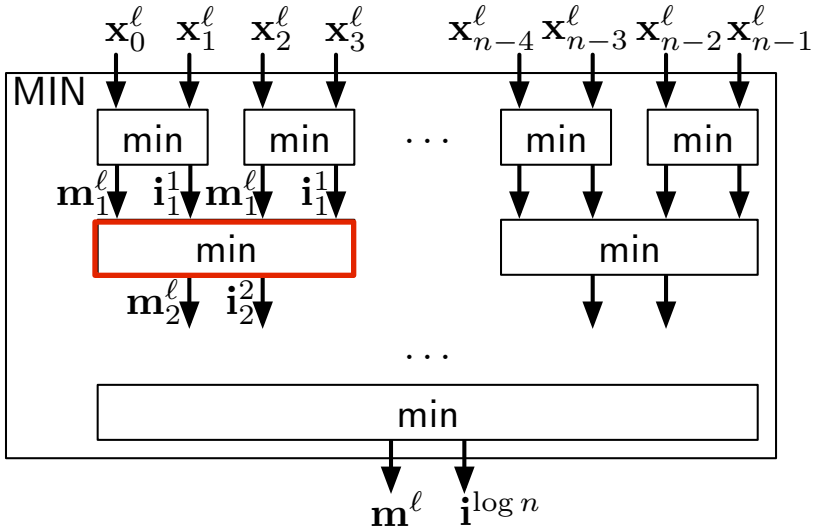
	Input	Output
Private $\mathcal{S} : x$	$\ell t'$ bits	ℓ bits
Private $\mathcal{C} : x$	$\mathsf{OT}^{\ell}_{t'}$	ℓ bits
HE $\mathcal{S} : \mathsf{Enc}(x)$	1 ciphertext + $5\ell t'$ bits + $\mathsf{OT}^{\ell}_{t'}$	1 ciphertext + $(\ell + \sigma)(5t' + 1)$ bits

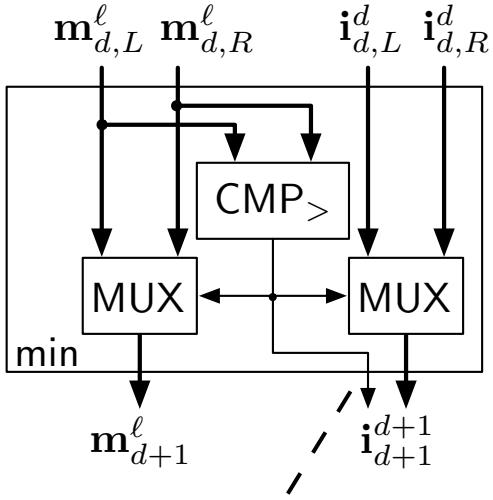
add random mask under HE and subtract in GC

add random mask in GC and subtract under HE

Efficient Circuit Constructions

Functionality for ℓ-bit Values	Size [# non-XOR gates]
Multiplexer, Addition, Subtraction, Comparison	ℓ
Multiplication (school method)	$2\ell^2 - \ell$
Minimum Value + Index of n values	$2\ell(n-1) + (n+1)$





reduces by $\approx n \log n$ non-XOR gates

Improved Application: Millionaire's Problem

GC is efficient secure comparison protocol [Yao86]

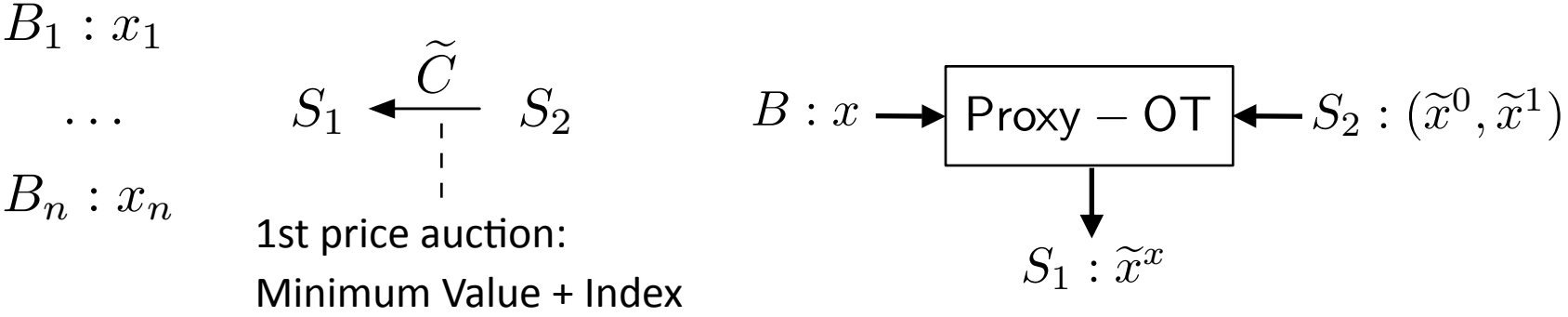
- **Communication Complexity:**

Communication Complexity	Previous Work (HE) [Fis01]	[BK04]	[DGK07]	This Work (GC) Setup Phase	Online Phase	Total
Asymptotic	$(\kappa+1)\ell T$	$4\ell T$	$2\ell T$	$16\ell t$	$3\ell t$	$19\ell t$
short-term	82 kByte	8 kByte	4 kByte	2.5 kByte	0.5 kByte	3.0 kByte
medium-term	164 kByte	16 kByte	8 kByte	3.5 kByte	0.7 kByte	4.2 kByte
long-term	246 kByte	24 kByte	12 kByte	4.0 kByte	0.8 kByte	4.8 kByte

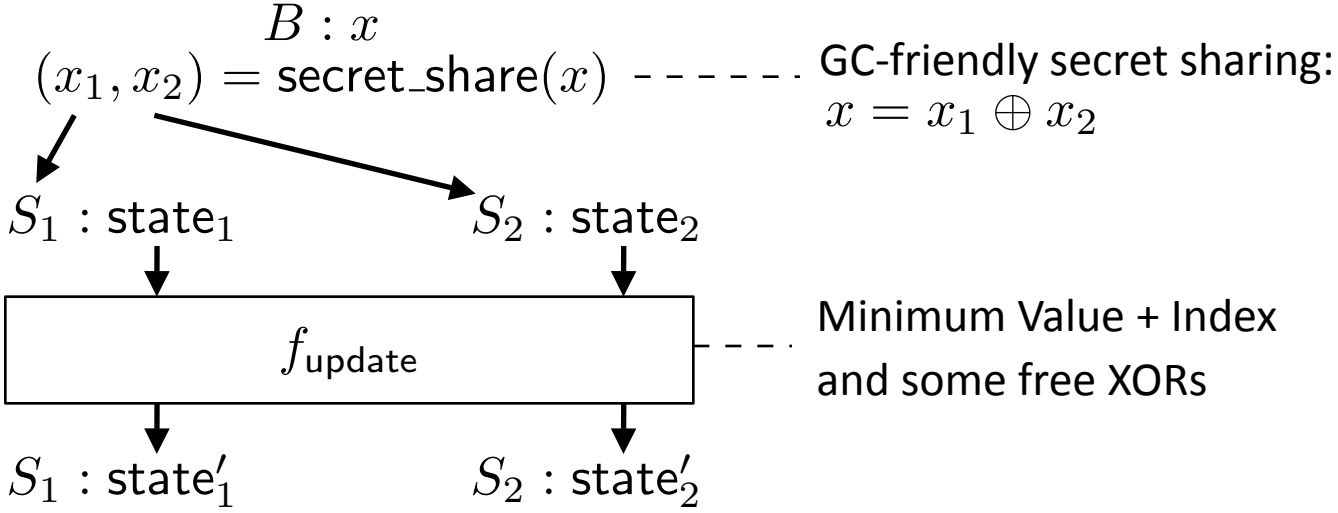
- **Computation Complexity:**
  OTs pre-computed in Setup Phase
  => **only** symmetric crypto in Online Phase!

Improved Application: Auctions

- **Offline Auctions** [NPS99]



- **Online Auctions**: [DGK07/08] with GC instead HE



Improved Application: Minimum Distance

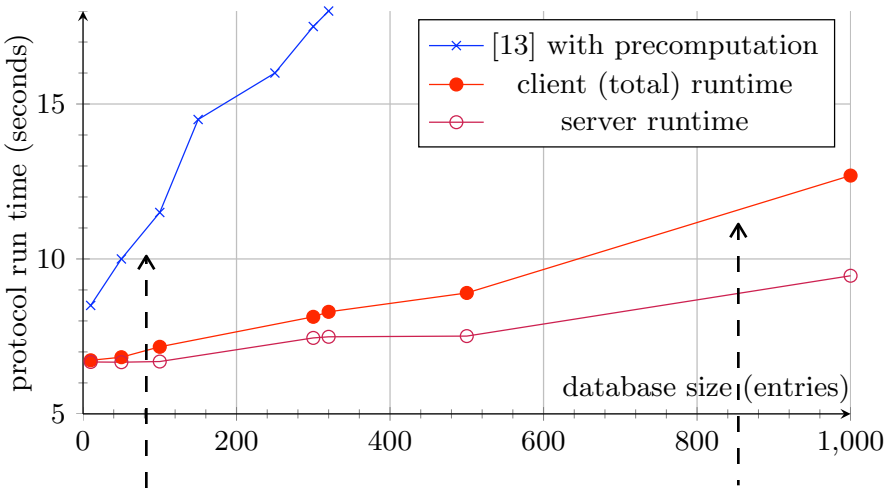
$\mathcal{C}$: query point P $\mathcal{S}$: points $Q_1, \ldots, Q_M$

$\mathcal{C}$: index min for $Q_{\min}$ closest to P

- Find index of closest point
  - Hamming distance $d_H(P,Q) = \sum p_i \oplus q_i = \bar{p}_i q_i + p_i \bar{q}_i$
  - Euclidean distance $d_E(P,Q)^2 = \sum_i^i (p_i - q_i)^2$
- Application: Biometric Authentication
  - Privacy-Preserving Face Recognition using Eigenfaces [EFGKLT09] (using HE only)
- Improved Approach: Combine HE with GC
  - HE to compute distances
  - GC to select minimum value+index

Improved Privacy-Preserving Face Recognition

Computation (online):



[EFGKLT09]: HE
implemented in **C++**
AMD Opteron 64, 2.4 GHz, 4GB

[SSW09]: Combine HE + GC
implemented in **Python**
AMD Athlon 64, 2.4 GHz, 4GB

Communication (online):

Protocol	HE §4.2 [13]			Hybrid §5.1 (Improvement)		
Round Complexity [moves]	$6\lceil\log(M+1)\rceil+4$			6 $(\mathcal{O}(\log M) \rightarrow \mathcal{O}(1))$		
Security Level	Short	Medium	Long	Short	Medium	Long
Asymptotic Communication Complexity (online)						
Projection [MB]	2.5	5.0	7.5	2.5	5.0	7.5
Distance [kB]	3.2	6.5	9.8	0.75 (23%)	1.0 (15%)	1.5 (15%)
Minimum [kB per face in DB]	15	29	44	0.99 (6.6%)	1.4 (4.8%)	1.6 (3.6%)

Thanks for your kind attention.

Contact:
thomas.schneider@trust.rub.de

Full Version:
http://eprint.iacr.org/2009/411

To be published in:
8th International Conference on Cryptology And Network Security (CANS'09)
December 14-16, 2009 - Kanazawa, Ishikawa, Japan